UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/578,892	05/11/2006	Toshihisa Nakano	2006_0706A	3449

52349 7590 04/28/2010

WENDEROTH, LIND & PONACK L.L.P.
1030 15th Street, N.W.
Suite 400 East
Washington, DC 20005-1503

EXAMINER	
KHOSHNOODI, NADIA	
ART UNIT	PAPER NUMBER
2437	

NOTIFICATION DATE	DELIVERY MODE
04/28/2010	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ddalecki@wenderoth.com
eoa@wenderoth.com

Office Action Summary	Application No.	Applicant(s)	
	10/578,892	NAKANO ET AL.	
	Examiner	Art Unit	
	NADIA KHOSHNOODI	2437	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _____.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-36,39,40 and 42* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-36, 39-40, and 42* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *11 May 2006* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

Applicant's arguments/amendments with respect to pending claims 1-36, 39-40, and 42 filed 1/27/2010 have been fully considered and therefore the claims are rejected under new grounds. The Examiner would like to point out that this action is made final (See MPEP 706.07a).

Claim Rejections - 35 USC § 112

I. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

II. Claims 1-36, 39-40 and 42 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Applicants have amended these claims to recite "pieces of new unique information" where previously the claims recited "pieces of derivative unique information." It seems that creating new pieces of unique information is in direct contrast with creating derivative pieces of unique information. Thus, Examiner reviewed Applicant's disclosure to determine the scope of the phrase "pieces of new unique information" however noticed that the Specification makes no reference to pieces of new unique information, it only refers to pieces of derivative unique information. As such, there seems to be no support for this particular amendment filed in Applicant's disclosure and "pieces of new unique information" lacks antecedent basis from the Specification. Applicants are invited to point out areas where they feel support the amendment

of this limitation, if there is such support. For Examination purposes Examiner has interpreted the limitation to the best of her ability in order to treat these claims on their merits, however if Applicants are unable to provide support, the scope of the claims will change if the limitation is further amended. Examiner further requests that Applicants provide support for all amendments made in order to ensure that the limitations, as amended, in the claims are fully supportive by the Specification.

Claim Rejections - 35 USC § 103

III. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

IV. Claims 1-36, 39-40, and 42 are rejected under 35 U.S.C. 103(a) as being unpatentable over Asano, US Patent No. 7,088,822 and further in view of Lotspiech et al., US Patent No. 7,010,125.

As per claims 1, 25, 40, and 42:

Asano teaches a management apparatus/copyright protection system/method/program/recording medium, the management apparatus/copyright protection system/method/program/recording medium comprising: a subset generating unit operable to calculate and generate, for each of nodes in layers except for the leaves of the tree structure, a subset being made up of one or more apparatus identifiers positioned subordinate to the node

(col. 12, lines 63-66 and col. 19, line 59 – col. 20, line 31); a first association unit operable to search, with respect to a node positioned in a lowermost layer other than a leaf layer, for a subset that wholly contains another subset from among the subsets generated by the subset generating unit for a parent node of the node positioned in an immediate upper layer thereof (col. 20, lines 28-42); a second association unit operable to search for another subset that wholly contains the containing subset, from among one or more other subsets generated for a node for which the subset was generated, and a plurality of subsets positioned in an immediate upper layer thereof and generated by the subset generating unit for a parent node of the node (col. 20, lines 2-65); a first control unit operable to control the second association unit so that processing thereof is repeatedly performed up to an uppermost layer (col. 21, lines 51-67); a second control unit operable to control the first association unit, the second association unit, and the first control unit so that processings thereof are repeatedly performed on all subsets generated for respective nodes in the lowermost layer (col. 21, lines 4-50); a first assignment unit operable to bring pieces of unique information into correspondence respectively with the subsets generated for respective nodes in the lowermost layer, and to assign each piece of unique information to apparatus identifiers contained in the corresponding subset in the lowermost layer (col. 12, lines 62-66 and col. 22, line 51- col. 23, line 10); and a second assignment unit operable to bring, for a subset being an association source generated for a node in one of the layers and one or more subsets being association destinations positioned in an immediately upper layer thereof and generated for a parent node of the node, pieces of unique information into correspondence respectively with the one or more subsets being association destinations and to assign the pieces of unique information being obtained by performing a prescribed operation on pieces of unique

information corresponding to the subset being an association source to generate corresponding decryption keys and the pieces of unique information (col. 28, lines 5-44).

Not explicitly disclosed is wherein the pieces of unique information are pieces of new unique information, associating the another subset as an association source with the subset as an association destination, and associating the subset as a new association source with another subset as a new association destination. However, Lotspiech et al. teach a system for tracing traitors and revoking access to a subset R of receivers if they are not authorized to receive the broadcasted content, where in order to perform this revocation, each subset is labeled with unique information (col. 4, line 45 - col. 5, line 29 and col. 8, lines 35-47). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Asano to provide a piece of new unique information to a subset and associate subsets with association source and destination information in order to group the subset of receivers that are unauthorized to receive the distributed content so that revocation is simplified. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Lotspiech et al. suggest that labeling all nodes in a particular subset allows creating a subset key in a direct path in association with left/right children, where revocation of traitor receivers is made easier since the traitor receivers are associated with the same subset in col. 4, line 45 – col. 5, line 29 and col. 7, line 50 - col. 8, line 21.

As per claims 2 and 26:

Asano teaches the management apparatus of claims 1 and 25, wherein the subset that is searched for by the first association unit and wholly contains said another subset in the

lowermost layer is made up of a smallest number of elements, and the first association unit associates said another subset being a parent node with the searched subset being a child node (col. 19, line 59- col. 20, line 20), the subset that is searched for by the second association unit and wholly contains the containing subset being the association destination is made up of a smallest number of elements, and the second association unit associates the association destination subset being a parent node with the searched subset being a child node (col. 19, line 59 – col. 20, line 20), and the first control unit controls the second association unit so that processing thereof is performed repeatedly up to the uppermost layer and generates subset trees whose roots are the subsets in the lowermost layer (col. 20, lines 21-49).

As per claims 3 and 27:

Asano teaches the management apparatus of claims 2 and 26, wherein the first association unit controls the second association unit so that processings thereof are repeatedly performed up to the uppermost layer, using one or more subsets obtained by excluding one or more subsets having been associated from subsets positioned in upper layers of the lowermost layer and generates subset trees whose roots are the subsets in the lowermost layer (col. 28, lines 1-25).

As per claims 4 and 28:

Asano teaches the management apparatus of claims 3 and 27, wherein the second assignment unit generates the pieces of derivative unique information from the pieces of unique information, using a one-way function and brings the generated pieces of derivative unique information into correspondence with the extending subsets (col. 22, line 62 - col. 23, line 4).

As per claims 5 and 29:

Asano teaches the management apparatus of claims 4 and 28, further comprising: a unique information obtaining unit operable to obtain, in a case where a subset in which an identifier of a terminal apparatus being a distribution destination of a piece of unique information appears as an element for a first time exists on one or more paths from the roots to one or more leaves of the subset trees, one or more pieces of unique information being in correspondence with such a subset (col. 22, line 51 – col. 23, line 10); and a distributing unit operable to distribute, to the terminal apparatus being the distribution destination, one or more groups each being made up of a different one of the obtained pieces of unique information and set identification information that identifies the subset that is in correspondence with the piece of unique information (col. 28, lines 26-44).

As per claim 6:

Asano teaches the management apparatus of claim 5, wherein the unique information obtaining unit includes: a first obtaining unit operable to search for the subset in which the identifier of the terminal apparatus being the distribution destination appears as an element for the first time in the one or more paths from the roots to the one or more leaves of the subset trees and, in the case where such a subset has been detected and has not been obtained, to obtain the detected subset (col. 27, lines 55-67); a second obtaining unit operable to obtain the one or more pieces of unique information that are in correspondence with the subset obtained by the first obtaining unit (col. 28, lines 1-25); and a repetition controlling unit operable to control the first and second obtaining units so that processings thereof are repeatedly performed until all of the one or more paths are searched (col. 28, lines 26-44).

As per claims 7 and 30:

Asano teaches the management apparatus of claims 5 and 29, further comprising: a first storing unit having an area for storing subsets being constituent elements of the subset trees and pieces of unique information that are respectively in correspondence with the subsets (col. 27, lines 31-54); a second storing unit having an area for storing a plurality of nodes constituting the subset trees and child nodes of the plurality of nodes (col. 27, lines 55-67); a first writing unit operable to write the subsets and the pieces of unique information into the first storing unit, while the subsets are brought into correspondence with the pieces unique information (col. 28, lines 1-25); and a second writing unit operable to write the plurality of nodes and the child nodes of the plurality of nodes into the second storing unit, while the nodes are brought into correspondence with the child nodes (col. 28, lines 16-38).

As per claim 8:

Asano teaches the management apparatus of claim 7, wherein the first storing unit has a first table storing therein a plurality of groups each being made up of a different one of the subsets and the corresponding piece of unique information, the second storing unit has a second table storing therein a plurality of groups each being made up of a different one of the nodes and the corresponding child node, the first writing unit writes the groups made up of the subsets and the corresponding pieces of unique information into the first table, and the second writing unit writes the groups made up of the nodes and the child nodes into the second storing unit (col. 28, lines 5-38).

As per claims 9 and 31:

Asano teaches the management apparatus of claim 7 and 30, wherein the second control unit generates a plurality of subset trees by controlling the first association unit, the second

association unit, and the first control unit so that the processings thereof are repeatedly performed on all the subsets in the lowermost layer, the first storing unit stores therein subsets contained in the plurality of subset trees and pieces of unique information that are in correspondence with the contained subsets (col. 28, lines 16-38), and the management apparatus further comprises: a revoked identifier storing unit having an area for storing one or more revoked identifiers indicating one or more revoked terminal apparatuses out of the plurality of terminal apparatuses (col. 28, line 59 - col. 29, line 22); an encryption key generating unit operable to obtain one or more of the subsets from the first storing unit based on what is stored in the revoked identifier storing unit, to obtain one or more encryption keys based on pieces of unique information that are respectively in correspondence with the obtained subsets, to encrypt a media key used for utilization of a content with the obtained encryption keys individually, so as to generate encrypted media keys that are equal in number to the one or more encryption keys (col. 29, lines 3-43); and a third writing unit operable to write, onto a recording medium mounted on the management apparatus, one or more groups each being made up of a different one of the encrypted media keys and a piece of reference identification information for identifying a subset used for obtaining the encryption key for the encrypted media key (col. 29, lines 31-43).

As per claims 10 and 32:

Asano teaches the management apparatus of claim 9 and 31 further comprising: a revoked identifier receiving unit operable to receive each revoked identifier and write the received revoked identifier into the revoked identifier storing unit (col. 30, lines 58-63).

As per claims 11 and 33:

Asano teaches the management apparatus of claims 9 and 31, wherein the encryption keys are each a common key and are identical to the decryption keys (col. 23, lines 55-67), the one-way function is further used for generating common keys based on the pieces of unique information from the pieces of unique information (col. 23, lines 1-54), and the encryption key generating unit includes: a subset obtaining unit operable to obtain, from the first storing unit, a subset that contains a largest number of one or more unrevoked identifiers which are other than the revoked identifiers stored in the revoked identifier storing unit (col. 29, line 3 - col. 30, line 9); a control unit operable to control the subset obtaining unit so that processing thereof is repeatedly performed until each of all the unrevoked identifiers belongs to any one of the one or more subsets obtained by the subset obtaining unit (col. 30, lines 6-33); a common key obtaining unit operable to obtain, using the one-way function, one or more common keys generated from the pieces of unique information that are respectively in correspondence with the subsets obtained by the subset obtaining unit (col. 33, line 6 – col. 34, line 6); and an encrypting unit operable to generate encrypted media keys that are equal in number to the common keys, using the common keys obtained by the common key obtaining unit (col. 34, lines 7-40).

As per claim 12:

Asano teaches the management apparatus of claim 9, wherein each piece of reference identification information is a corresponding subset used for obtaining a corresponding common key for the encrypted media key, the third writing unit writes, onto the recording medium, one or more groups each being made up of a different one of the encrypted media keys and the corresponding subset used for obtaining the corresponding common key for the encrypted media key (col. 34, lines 40-51), the distributing unit distributes, to the terminal apparatus being the

distribution destination, one or more groups each being made up of a different one of the obtained pieces of unique information and a piece of set identification information that is one of the subsets with which the piece of unique information is in correspondence (col. 34, lines 2-61 and col. 32, lines 1-11), and the distributing unit further distributes a data structure indicating the subset trees (col. 32, lines 20-49).

As per claim 13:

Asano teaches the management apparatus of claim 9, further comprising: a path information obtaining unit operable to obtain a piece of path information including (i) a generation path indicating, for each subset, a path that extends from a root subset being a root of a subset tree to which the subset belongs and reaches the subset (col. 28, lines 26-44), and (ii) a root identifier indicating the root subset, wherein the reference identification information is a piece of path information for the subset used for obtaining the encryption key for the encrypted media key (col. 29, lines 1-18), the third writing unit writes, onto the recording medium, one or more groups each being made up of a different one of the encrypted media keys and a piece of path information for the subset used for obtaining the encryption key for the encrypted media key (col. 29, lines 19-30), and the distributing unit distributes, to the terminal apparatus being the distribution destination, one or more groups each being made up of a different one of the obtained pieces of unique information and a piece of set identification information that is a piece of path information for the subset with which the obtained piece of unique information is in correspondence (col. 29, line 31 – col. 30, line 43).

As per claim 14:

Asano teaches a terminal apparatus to which a piece of unique information being a base of a decryption key for decrypting a piece of encrypted data is assigned by a management apparatus that manages, with use of a tree structure, a plurality of apparatus identifiers identifying a plurality of terminal apparatuses, wherein the management apparatus (i) calculates and generates, for each of nodes in layers except for leaves of the tree structure, a subset defined as a set being made up of one or more apparatus identifiers positioned subordinate to the node (col. 12, lines 62-66 and col. 19, line 59 – col. 20, line 31), (ii) searches, with respect to a node, positioned in a lowermost layer other than a leaf layer, for a subset that wholly contains another subset from among a plurality of subsets generated by the subset generating unit for a parent node of the node positioned in an immediately upper layer thereof (col. 20, lines 28-42), (iii) searches for another subset that wholly contains the containing subset being an association destination, from among one or more other subsets generated for a node for which the subset was generated, and a plurality of subsets positioned in an immediate upper layer thereof and generated by the subset generating unit for a parent node of the node (col. 20, lines 28-42), (iv) controls a second association unit so that the associating is repeatedly performed up to an uppermost layer (col. 21, lines 51-67), (v) performs control so that the first association, second association, and the control on the second association unit are repeatedly performed on all subsets generated for respective nodes in the lowermost layer (col. 21, lines 4-50), (vi) performs a first assignment for bringing pieces of unique information into correspondence respectively with the subsets generated for respective nodes in the lowermost layer and to assign each piece of unique information to apparatus identifiers contained in the corresponding subset in the lowermost layer (col. 12, lines 62-66 and col. 22, line 51- col. 23, line 10, and (vii) performs a

second assignment for bringing pieces of unique information into correspondence respectively with the one or more subsets, and to assign the piece of unique information to apparatus identifiers contained in one or more subsets, the pieces of unique information being obtained by performing a prescribed operation on pieces of unique information corresponding to the subset being an association source to generate corresponding decryption keys and the pieces of unique information (col. 28, lines 5-44), and the terminal apparatus includes a unique information storing unit storing therein a piece of unique information that contains an apparatus identifier of the terminal apparatus, out of the pieces of unique information that have been distributed from the management apparatus in advance and are brought into correspondence with the subsets (col. 20, line 21-65).

Not explicitly disclosed is performs a first association for associating another subset as an association source with the subset as an association destination; performing a second association for associating the subset as a new association source with another subset as a new association destination; and wherein pieces of new unique information are included in a subset being an association source generated for a node in one of the layers and one or more subsets being association destinations positioned in an immediately upper layer thereof and generated for a parent node of the node. However, Lotspiech et al. teach a system for tracing traitors and revoking access to a subset R of receivers if they are not authorized to receive the broadcasted content, where in order to perform this revocation, each subset is labeled with unique information (col. 4, line 45 - col. 5, line 29 and col. 8, lines 35-47). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Asano to provide a piece of new unique information to a subset and associate

subsets with association source and destination information in order to group the subset of receivers that are unauthorized to receive the distributed content so that revocation is simplified. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Lotspiech et al. suggest that labeling all nodes in a particular subset allows creating a subset key in a direct path in association with left/right children, where revocation of traitor receivers is made easier since the traitor receivers are associated with the same subset in col. 4, line 45 – col. 5, line 29 and col. 7, line 50 - col. 8, line 21.

As per claim 15:

Asano teaches the terminal apparatus of claim 14, wherein the unique information storing unit further stores therein a piece of set identification information identifying a subset with which the stored piece of unique information is in correspondence, and the terminal apparatus further includes: a judging unit operable to judge whether the piece of set identification information indicates that the terminal apparatus is an unrevoked apparatus (col. 27, lines 3-54); a first obtaining unit operable to, in a case where a judgment result of the judgment unit is in the affirmative, obtain an encrypted media key that (i) is obtained by encrypting a media key with an encryption key based on a specific piece of unique information out of the pieces of unique information in correspondence with the subsets generated by the management apparatus and (ii) is in correspondence with a piece of key related information related to the encryption key (col. 27, line 55 – col. 28, line 25 and col. 29, line 31 - col. 30, line 32); a second obtaining unit operable to obtain a decryption key that is in correspondence with the encryption key using the piece of unique information stored in the unique information storing unit (col. 28, lines 26-64);

and a decrypting unit operable to decrypt the encrypted media key obtained by the first obtaining unit, using the decryption key obtained by the second obtaining unit, so as to generate the media key (col. 30, line 33-57).

As per claim 16:

Asano teaches the terminal apparatus of claim 15, wherein the specific piece of unique information is a piece of reference unique information that is in correspondence with a subset that contains, at a time when the encrypted media key is generated, one or more identifiers of one or more unrevoked apparatuses (col. 19, line 59 – col. 20, line 67), the encryption key is a common key, the piece of key related information is a piece of reference identification information that identifies the subset with which the piece of reference unique information is in correspondence, the encrypted media key is in correspondence with the piece of reference identification information (col. 21, lines 1-50), the judgment unit judges that the piece of set identification information indicates that the terminal apparatus is an unrevoked apparatus, in a case where a path exists that extends from the subset identified by the piece of set identification information stored in the unique information storing unit and reaches the subset identified by the piece of reference identification information (col. 27, lines 30-54), the first obtaining unit obtains the encrypted media key that is encrypted by an encryption key based on the piece of reference unique information in correspondence with the piece of reference identification information (col. 21, lines 25-67), the second obtaining unit obtains the decryption key and takes the obtained decryption key as the common key, and the decrypting unit decrypts the encrypted media key, using the obtained common key (col. 22, lines 1-42).

As per claim 17:

Asano teaches the terminal apparatus of claim 16, wherein the management apparatus (i) searches for a subset that wholly contains said another subset in the lowermost layer and is made up of a smallest number of elements and associates said another subset being a parent node with the searched subset being a child node (col. 19, line 59 - col. 20, line 20), (ii) further searches for a subset that wholly contains the containing subset being an association destination, is made up of a smallest number of elements, and has not been associated yet, and associates the association destination subset being a parent node with the further searched subset being a child node, so as to generate subset trees whose roots are the subsets in the lowermost layer (col. 19, line 59 - col. 20, line 20), the unique information storing unit further stores therein a data structure for constituting the subset trees generated by the management apparatus, and the judgment unit judges, using the subset trees constituted with the data structure, whether or not a path exists that extends from the subset that is in correspondence with the piece of unique information stored in the unique information storing unit and reaches the subset identified by the piece of reference identification information (col. 30, lines 10-57).

As per claim 18:

Asano teaches the terminal apparatus of claim 16, wherein the management apparatus (i) searches for a subset that wholly contains said another subset in the lowermost layer and is made up of a smallest number of elements and associates said another subset being a parent node with the searched subset being a child node, (ii) further searches for a subset that wholly contains the containing subset being an association destination, is made up of a smallest number of elements, and has not been associated yet, and associates the association destination subset being a parent node with the further searched subset being a child node, so as to generate subset trees whose

roots are the subsets in the lowermost layer (col. 19, line 59 – col. 20, line 20), the piece of reference identification information includes a first generation path that extends from a root of one of the subset trees and reaches a reference subset with which the piece of reference unique information is in correspondence (col. 29, lines 3-18), the piece of set identification information includes a second generation path that extends from the root of the one of the subset trees and reaches a subset with which the piece of unique information is in correspondence (col. 29, lines 19-54), and the judgment unit judges, in a case where the second generation path is contained in the first generation path, that a path exists that extends from the subset identified by the piece of set identification information and reaches the subset identified by the piece of reference identification information (col. 30, lines 10-64).

As per claim 19:

Asano teaches the terminal apparatus of claim 16, wherein the management apparatus (i) inputs a piece of unique information that is in correspondence with a subset to a one-way function so as to generate a common key based on the piece of unique information and generate a piece of derivative unique information deriving from the piece of unique information (col. 23, lines 1-54), (ii) brings the generated piece of derivative unique information into correspondence with a subset that is associated with the subset with which the inputted piece of unique information is in correspondence (col. 29, line 3 – col. 30, line 9), and (iii) assigns the generated piece of derivative unique information to apparatus identifiers included in the associated subset, the second obtaining unit includes: a device key obtaining unit operable to generate and obtain a device key based on the piece of unique information and the piece of derivative unique information from the piece of unique information stored in the unique information storing unit,

using a function identical to the one-way function (col. 23, lines 1-54); a repetition unit operable to control the device key obtaining unit so that processing thereof is repeatedly performed using each piece of unique information obtained by the device key obtaining unit as a next input to the identical function, until a device key based on the piece of reference unique information is obtained (col. 30, lines 10-33); and a decryption key obtaining unit operable to obtain, as the common key, the device key based on the piece of reference unique information obtained by the device key obtaining unit (col. 33, line 6 - col. 34, line 6).

As per claim 20:

Asano teaches the terminal apparatus of claim 19, further comprising: a content obtaining unit operable to obtain a content; a content key obtaining unit operable to obtain a content key; a first encrypting unit operable to encrypt the content key obtained by the content key obtaining unit, using the media key obtained by the decrypting unit so as to generate an encrypted content key; a second encrypting unit operable to encrypt the content obtained by the content obtaining unit, using the content key obtained by the content key obtaining unit so as to generate an encrypted content; and a writing unit operable to write the encrypted content key and the encrypted content into a recording medium (col. 29, line 55 – col. 31, line 45).

As per claim 21:

Asano teaches the terminal apparatus of claim 20, wherein the writing unit writes the encrypted content key and the encrypted content into the recording medium which is included in an apparatus located in a network, via a communication medium (col. 12, line 54 – col. 13, line 65).

As per claim 22:

Asano teaches the terminal apparatus of claim 19, further comprising: an encrypted content key obtaining unit operable to obtain an encrypted content key which is obtained by encrypting a content key with the media key; an encrypted content obtaining unit operable to obtain an encrypted content which is obtained by encrypting a content with the content key; a first decrypting unit operable to decrypt the encrypted content key obtained by the encrypted content key obtaining unit, using the media key so as to generate the content key; a second decrypting unit operable to decrypt the encrypted content obtained by the encrypted content obtaining unit, using the content key so as to generate the content; and a playback unit operable to play back the content generated by the second decrypting unit (col. 29, line 55 – col. 31, line 45).

As per claim 23:

Asano teaches the terminal apparatus of claim 22, wherein the encrypted content key and the encrypted content are recorded on a recording medium, which is mounted on the terminal apparatus, the encrypted content key obtaining unit obtains the encrypted content key from the recording medium, and the encrypted content obtaining unit obtains the content from the recording medium (col. 13, line 57 - col. 14, line 60).

As per claim 24:

Asano teaches the terminal apparatus of claim 22, wherein the encrypted content obtaining unit obtains the encrypted content key via a communication medium, and the encrypted content obtaining unit obtains the content via a communication medium (col. 17, line 1-39 and col. 20, lines 50-65).

As per claim 34:

Asano teaches the copyright protection system of claim 33, wherein the terminal apparatus comprises: a unique information storing unit storing therein one or more groups each being made up of a piece of unique information distributed from the distributing unit of the management apparatus in advance and a piece of set identification information identifying a subset with which the piece of unique information is in correspondence (col. 19, line 59 – col. 20, line 65); a judging unit operable to judge whether the piece of set identification information indicates that the terminal apparatus is an unrevoked apparatus; a first obtaining unit operable to, in a case where a judgment result of the judgment unit is in the affirmative, obtain one encrypted media key from the recording medium; a second obtaining unit operable to obtain a decryption key that is in correspondence with the encryption key, using the piece of unique information stored in the unique information storing unit; and a decrypting unit operable to decrypt the encrypted media key obtained by the first obtaining unit, using the decryption key obtained by the second obtaining unit, so as to generate the media key (col. 27, line 55 – col. 28, line 25 and col. 29, line 31 - col. 30, line 32 and col. 30, lines 33-57).

As per claim 35:

Asano teaches the copyright protection system of claim 34, wherein the encryption key is a common key, the judgment unit judges that the piece of set identification information indicates that the terminal apparatus is an unrevoked apparatus, in a case where a path exists that extends from the subset being stored in the unique information storing unit and being identified by the piece of set identification information stored in the unique information storing unit and reaches the subset identified by the piece of reference identification information (col. 27, lines 30-54), the first obtaining unit obtains an encrypted media key that is in correspondence with the piece of

reference identification information (col. 21, lines 25-67), the second obtaining unit obtains the decryption key and takes the obtained decryption key as the common key, and the decrypting unit decrypts the encrypted media key, using the obtained common key (col. 22, lines 1-42).

As per claim 36:

Asano teaches the copyright protection system of claim 35, wherein the second obtaining unit includes: a device key obtaining unit operable to generate and obtain a device key based on the piece of unique information and the piece of derivative unique information from the piece of unique information stored in the unique information storing unit, using a function identical to the one-way function (col. 23, lines 1-54); a repetition unit operable to control the device key obtaining unit so that processing thereof is repeatedly performed using each piece of unique information obtained by the device key obtaining unit as a next input to the identical function, until a device key based on the piece of reference unique information is obtained (col. 21, lines 25-67); and a decryption key obtaining unit operable to obtain, as the common key, the device key based on the piece of reference unique information obtained by the device key obtaining unit (col. 22, lines 1-42).

As per claim 39:

Asano teaches a management apparatus, the management apparatus comprising: a subset generating unit operable to calculate and generate, for each of nodes in layers except for the leaves of the tree structure, a subset defined as being made up of one or more apparatus identifiers positioned subordinate to the node (col. 12, lines 62-66 and col. 19, line 59 – col. 20, line 31); a group generating unit operable to select, out of subsets positioned in a layer, and put into one group (i) a subset that contains a smallest number of elements and (ii) another subset

that contains the subset containing the smallest number of elements (col. 20, lines 28-65); a first control unit operable to control the group generating unit so that processing thereof is repeatedly performed on all subsets each of which is positioned in the layer and contains the smallest number of elements (col. 29, line 3 - col. 30, line 9); a second control unit operable to control the group generating unit and the first control unit so that processings thereof are repeatedly performed on all of layers (col. 30, lines 10-33); an integrating unit operable to, after the second control unit performs the processing on all of the layers, integrate into one group (i) a lower-layer group and (ii) an upper-layer group that includes a subset that wholly contains one of subsets belonging to the lower-layer group and that is generated for a parent node of a node for which the one of subsets are generated, the lower-layer group and the upper-layer group belonging to mutually different layers (col. 21, lines 4-67); a first assignment unit operable to, after groups are integrated in all of the layers, bring pieces of unique information into correspondence with subsets each of which has a smallest number of elements in each of remaining groups and assign each piece of unique information to one or more apparatus identifiers contained in the corresponding subset (col. 12, lines 62-66 and col. 22, line 51- col. 23, line 10); and a second assignment unit operable to bring pieces of derivative unique information into correspondence with subsets other than the subset that has the smallest number of elements respectively and assigns each piece of unique information to one or more apparatus identifiers that are contained in each of said other subsets (col. 28, lines 5-44).

Not explicitly disclosed is wherein the second assignment unit assigns new unique information to one or more apparatus identifiers and wherein the new unique information is obtained by performing a prescribed operation on pieces of unique information corresponding to

the subset that has the smallest number of elements respectively to generate corresponding decryption keys and pieces of new unique information. However, Lotspiech et al. teach a system for tracing traitors and revoking access to a subset R of receivers if they are not authorized to receive the broadcasted content, where in order to perform this revocation, each subset is labeled with unique information (col. 4, line 45 - col. 5, line 29 and col. 8, lines 35-47). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Asano to provide a piece of new unique information to a subset and associate subsets with association source and destination information in order to group the subset of receivers that are unauthorized to receive the distributed content so that revocation is simplified. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Lotspiech et al. suggest that labeling all nodes in a particular subset allows creating a subset key in a direct path in association with left/right children, where revocation of traitor receivers is made easier since the traitor receivers are associated with the same subset in col. 4, line 45 – col. 5, line 29 and col. 7, line 50 - col. 8, line 21.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO

MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Nadia Khoshnoodi whose telephone number is (571) 272-3825. The examiner can normally be reached on M-F: 8:00-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

/Nadia Khoshnoodi/
Examiner, Art Unit 2437
4/24/2010

NK

/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2437